# Enterprise-Grade Virtual Conference Platform Infrastructure

At 6Connex, there is no higher priority than the privacy and security of our customers' data. We lead the industry as a trusted repository for customer data through an enterprise-class privacy program and provide a secure infrastructure and flexible tools that help enable our customers to comply with global privacy and data protection regulations.

- **Secure Registration and Passwords** - All attendee registration info is protected by SSL and encrypted again in the DB utilizing SHA256.

- **Secure Cookies & Storage** - All cookies are transmitting with HTTPS only

- **Unique Certification Authentication** - with each client

- **Secure access** – Customer access points, also called API endpoints, allow secure HTTP access (HTTPS) so that secure communication sessions with 6Connex use SSL/TLS.

- **Firewalls** – 6Connex controls how accessible our instances are by configuring built-in firewall rules – from totally public to completely private, or somewhere in between.

- **Encrypted data storage** – 6Connex customer data and objects stored in Amazon EBS, Amazon S3, and SQL Server RDS are encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys. 6Connex uses AWS Key Management Service (KMS) to create and manage keys and control the use of encryption across all our AWS services. AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to protect 6Connex's keys.

- **Perfect Forward Secrecy** – For even greater communication privacy, the 6Connex platform is behind Elastic Load Balancers to offer newer, stronger cipher suites. These cipher suites allow 6Connex (in SSL/TLS) to use Perfect Forward Secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.

- **Centralized key management** –6Connex uses AWS Key Management Service (KMS) to create and manage keys and control the use of encryption across all our AWS services. AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to protect 6Connex's keys.

- **Amazon Relational Database Service (Amazon RDS)** - This give 6Connex a highly robust replication process and enhanced availability and reliability in our databases.

| Question | Answer |
|---|---|
| **In detail, please provide the minimum laptop/desktop software requirements needed to be operational on the 6Connex Platform.** | The 6Connex platform is a multi-platform cloud-based application that will run on your PC, MAC and mobile device with in any modern browser. The 6Connex platform works best on: <br><br>Internet Explorer 8+ <br>All recent versions of Google Chrome <br>Safari 5.0+ <br>Firefox 3.6+ <br><br>The 6Connex platform is also accessible via several mobile devices: <br>iPhone/iPad Safari/iOs 5.1+ <br><br>Android Phone/Tablet - OS 2.3 or higher <br> Chrome/Native Browser 2.3+ <br><br>Windows Tablet <br> IE 10+ |

| Operating System | Processor | RAM | Internet Browser | Hardware | Media P |
|---|---|---|---|---|---|
| Windows 10 <br>Windows 8.1 + Pro <br>Windows 7 <br>Android 4.4+ <br>Apple Max OS X 10.9+ <br>Apple IOS 8.4+ | 1GHz | 1GB | Internet Explorer 9+ <br><br>All recent versions of Google Chrome <br><br>Safari 5.0+ <br><br>Firefox 3.6+ <br><br>iPhone/iPad - Safari/iOs 5.1+ <br><br>Android Phone/Tablet - OS 2.3 or higher, Chrome, Native Browser 2.3+ <br><br>Windows Tablet - IE 10+ | Audio: Sound Card with Speakers <br><br>Video: Screen with 1024x768+ resolution support | HTML5 Streamin enabled <br><br>Apple iO streamin enabled <br><br>Android streamin enabled |

| | |
|---|---|
| **What is the 6Connex Platform written in?** | 6Connex software is based on HTML5 technology (not Flash). No software download required. Both PC and MAC operating system supported as well as mobile devices. |
| **Where is your data center hosting the platform located?** | 6Connex offers the choice of hosting in Amazon Web Services data centers in either Germany (Europe hosts) or North America (US & Canada hosts). |
| **Do you support AES-256 encryption for data storage?** | Yes. Cryptography used in our system.<br>Attendee<br>   Password - SHA-256 with salt<br>   Personal data - AES-256 (Advanced Encryption Standard)<br>Admin<br>   Password - SHA-256 with salt |
| **Is your platform ISO 27001 compliant?** | Yes. 6Connex is the only virtual conference platform that is ISO 27001 certified. This means that our technology, systems, processes and controls meet the highest data security standard. It also means that a 3rd party firm audits us annually to confirm all of this and we have to recertify completely every three years. |

| | |
|---|---|
| **The 6Connex Environments and maintenance windows.** | All 6Connexclients are provided a testing (Test) and production (Prod) environment. Clients are given access to our staging environments 4-5 weeks prior to implementation to test all new enhancements. 6Connex provides clients with a true SaaS multi-tenanted environment.  Therefore, all new features clients are not given approval rights to bypass an enhancement.<br><br>Availability<br>Platform availability is vital to 6Connex. With Amazon Web Services (AWS), the 6Connex platform has a level agreement which gives us a commitment of 99.978% uptime. AWS utilizes an end-to-end approach to secure and harden their infrastructure, including physical, operational, and software measures. The 6Connex Platform Team follows industry standard operations.<br><br>Recovery<br>6Connex uses the AWS cloud to enable faster disaster recovery of their critical IT systems. 6Connex has a "hot standby" environment that provides a rapid failover. To ensure continuity 6Connex performs quarterly disaster recovery tests and the plans are reviewed and updated after each test.<br><br>Maintenance<br>The 6Conned platform uses a custom automated patch management solution to "hot patch" our platform. Using a controlled rollout, the 6Connex in-house solution groups systems and applications based on attributes like geographic location and functional use on the platform. These automated updates are tested on our testing platform before moving into staging where all updates are tested again. If the patch does not pass testing the patch is delayed. All updates are tested on a list of browsers, OSs, and devices. Regression testing is done for all updates. |
| **How protected is my data on the 6Connex Platform?** | All information transferred within the 6Connex platform is authenticated using asymmetric cryptography (SSL Data Transfers). All registration information is protected by SSL and encrypted again in the DB utilizing SHA256.  All cookies are transmitted with HttpOnly. For secure events, cookies are transmitted with HTTPS.<br><br>6Connex uses server-side encryption to encrypt data before it is written to disk. Each object is encrypted with a unique data key. This key is encrypted with a periodically rotated master key.  Server-side encryption uses 256-bit Advanced Encryption Standard (AES) keys for both object and master keys.<br><br>The 6Connex platform is multi-tenanted allowing client instances to have partitioned data and configuration. The platform contrasts with multi-instance architectures where separate software instances (or hardware systems) operate on behalf of different client organizations. All client data will be set up and configured within the 6Connex platform. |

| **Does 6Connex comply with Privacy and Data Protection Requirements?** | We have the only virtual conference platform that is ISO/IEC 27001 certified. The 6Connex platform is also General Data Protection Regulation (GDPR) compliant. This is a major differentiator vs. competing platforms. Event Hosts collect personal data on attendees so compliance with privacy laws is a must to avoid hefty fines and damaged reputation. |
| --- | --- |
| **How does 6Connex handle data integrity in the context completeness, accuracy and resistance to unauthorized modification or destruction?** | Compliance with data protection and privacy principles is based on cooperation between 6Connex and our customers. For example, 6Connex's contracts with our customers' state that customers are responsible for the accuracy, quality, integrity, reliability, and appropriateness of data submitted to the 6Connex platform and that customers must comply with applicable laws in using the 6Connex service.<br><br>6Connex maintains appropriate administrative, physical, and technical safeguards to help protect the security, confidentiality, and integrity of data our customers submit to the 6Connex platform as customer data. 6Connex's customers are responsible for ensuring the security of their customer data in their use of the service. |
| **Can the 6Connex platform scale to accommodate all my attendees?** | The 6Connex platform can scale high to support events with 30,000+ attendees no problem.<br><br>The 6Connex platform is hosted with Amazon Web Services (AWS). One core feature of AWS is its flexibility. All 6Connex services work and communicate together to automatically judge demand and handle the demand accordingly. The 6Connex platform runs behind Elastic Load Balancers that automatically scale its request handling capacity to meet the demands of application traffic. Additionally, AWS offers integration with Auto Scaling to ensure that the 6Connex Platform has back-end capacity to meet varying levels of traffic without requiring manual intervention.<br><br>By using Elastic Load Balancing the 6Connex platform achieves higher levels of fault tolerance during a client's experience by automatically routing traffic across multiple instances and multiple Availability Zones. Elastic Load Balancing ensures that only healthy server instances receive traffic by detecting unhealthy instances and rerouting traffic across the remaining healthy instances. If all 6Connex instances in one Availability Zone are unhealthy the Elastic Load Balancing will route traffic to our healthy platform instances in our other zones.<br><br>With every minor and major release, we test the platform's fault tolerance by stress testing the environment. During testing we closely monitor all network traffic and all services looking for bottlenecks that could lower traffic speeds and/or create unhealthy instances. With these findings we can update our code and/or deploy additional services to better respond to higher traffic. |

| | |
|---|---|
| **Are intrusion detection mechanisms applied to critical systems and to networks?** | 6Connex uses Core Impact Pro for our own penetration testing. 6Connex performs bi-annual penetration tests against all systems.<br><br>We have had a number of clients perform their own penetration testing on our platform. If a client would like to conduct a penetration test we will need the clients source IP addresses so we can open a request with AWS.  Once the request is granted the client will have a fixed amount of time to perform the test. We can also provide a number of virtual experiences to your Security/Trust teams to verify and test our platform. |
| **The 6Connex Issue Resolution process.** | 6Connex as a whole supports a quick response the moment a platform issue/security incident is recognized.<br><br>6Connex incident management process (High Level):<br><br>Incident detection and recording<br>Classification and initial support<br>Investigation and diagnosis<br>Resolution and recovery<br>Incident closure<br>Ownership, monitoring, tracking, and communication (monitoring the progress of the resolution of the incident and keeping those who are affected by the incident up to date with the status)<br><br>To reduce risks resulting from IT incidents 6Connex has monthly procedures and instructions for patch and vulnerability management. Management at 6Connex reviews all security incidents no matter the size.<br><br>6Connex has an ongoing client escalation distribution list (SPOC) used to contact clients during security incidents and report progress, status, and resolution.<br><br>All processes are documented and are reviewed annually as per our ISO-27001 certification. |
| **Are the 6Connex systems configured to capture and log successful and failed user authentication (login) attempts and user authorization failures?** | 6Connex does extensive monitoring to detect unauthorized information processing activities. The monitoring includes e.g. authorized access, all privileged operations, unauthorized access attempts, system alerts or failures, and changes to, or attempts to change, system security settings and controls. All logs are checked monthly and archived after. |

| | |
|---|---|
| **Does 6Connex retain system log files for a specified period of time to assist in access control monitoring and security investigations?** | 6Connex maintains application and service logs. Management at 6Connex reviews all security incidents no matter the size. Logging is configurable by the 6Connex super admin only.<br><br>6Connex applications and services logs are stored events from a single application or component rather than events that might have system wide impact. This category of logs includes four subtypes: Admin, Operational, Analytic, and Debug logs. Events in Admin logs are of particular interest to 6Connex when troubleshooting problems. Events in the Admin log provide 6Connex with guidance about how to respond to them. Events in the Operational log are also useful to 6Connexs, but they are likely to require more interpretation.<br><br>Analytic logs store events that trace an issue and, often, a high volume of events are logged. Debug logs are used by developers when debugging applications. |
| **What type of servers host the 6Connex Platform? (e.g. Apache, 64 bit, etc...)** | Tomcat running on 64-bit amazon Linux based on CENTOS |
| **What OS are the servers running? (e.g. Oracle Linux, 64 bit, etc...)** | Amazon Linux - based on CENTOS 64-bit architecture |

Additional resources available upon request:

- ✓ Third-party vulnerability scans and penetration test results from within the last 12 months
- ✓ 6Connex Data retention policy
- ✓ Security Policy documentation including: InfoSec policy, incident management, etc.